AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A cryptographic method for generating public and private keys in a device that is able to exchange messages on at least one communication channel, the private key being stored secretly in said device and the public key being broadcast publicly, the generation method comprising the following steps:

- selecting two prime numbers p and q which are distinct and of similar sizes;

- calculating the number n equal to the product of p and q;

~~- calculating the lowest common multiple of the numbers (p-1) and (q-1):~~

~~$\lambda(n)=LCM(p-1, q-1)$~~

- determining a number g, $0 \leq g < n^2$, which satisfies the following two conditions during the calculation of a cryptogram c, where $c=g^m \bmod n^2$ and m is a number representing a message with $0 \leq m < n$:

a) g is invertible modulo n^2, and

b) $ord(g,n^2) = 0 \bmod n$, ~~and~~

- selecting g = 2 if g satisfies said conditions a) and b);

~~wherein~~ generating the public key of said device ~~is formed by~~ from the parameters n and g; and

~~its~~ generating the private key ~~is formed by~~ from at least the parameters p and q.

2. (Currently Amended) A cryptographic communication system with public and private keys generated according to Claim 1, comprising a communication channel and first and second communicating devices, each device comprising at least one communication interface, data processing means and storage means, wherein ~~an encryption method is implemented in~~ said first device executes the following steps to send [[a]] the number m ~~representing a message, $0 \leq m < n$,~~ to said second device~~, said encryption method comprising the following steps:~~

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

- transmitting said cryptogram over the communication channel to the second device.

3. (Currently Amended) A system according to Claim 2, wherein said first device ~~implementing the encryption method~~ also comprises a generator for a random integer number r, and wherein said first device:

- performs the drawing of a random integer number r, and

- calculates the cryptogram c by performing the encryption calculation: $c = g^{m+nr} \bmod (n^2)$.

4. (Currently Amended) A system according to Claim 2, wherein said first device ~~implementing the encryption method~~ also comprises a generator for a random integer number r, and wherein said first device:

- performs the drawing of a random integer number r, and

- calculates the cryptogram c by performing the encryption calculation:

$c = g^m r^n \bmod (n^2)$.

5. (Currently Amended) A system according to Claim [[4]] 22, wherein said second device ~~implements a decryption method, in order~~ performs the following calculation to decrypt said cryptogram c~~, which comprises performing the calculation~~:

$m = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$

where, $\log_n(x) = \frac{x-1}{n}$

x being any integer.

6. (Currently Amended) A system according to Claim 5, wherein said second device ~~implementing said decryption method~~ precalculates the quantity:

$\alpha_{n.g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$

and stores it secretly in a protected area of a program memory.

7. (Currently Amended) A system according to Claim 5, wherein said second device performs the following calculation ~~steps during said decryption method~~, using the Chinese Remainder Theorem CRT:

$m_p = \log_p(c^{p-1} \bmod p^2).\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$.

$m_q = \log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$.

$m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

8. (Currently Amended) A system according to Claim 7, wherein said second device ~~implementing said decryption method~~ precalculates the following quantities

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$ and

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

and stores them secretly in a protected area of a program memory.

9. (Currently Amended) A cryptographic communication system with public and private keys generated according to Claim [[1]] 21, comprising a communication channel and first and second communicating devices, each device comprising a communication interface, data processing means and storage means, wherein ~~an encryption method is implemented in~~ said first device, executes the following steps to send the ~~for sending a~~ number m ~~representing a message, $0 \leq m < n^2$,~~ to said second device~~, said encryption method comprising the following steps~~:

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- performing the following calculations:

1. $m_1 = m \bmod n$

2. $m_2 = (m-m1)/n$

3. $c = g^{m1}\, m_2{}^n \bmod n^2$, and

- transmitting the cryptogram c over the communication channel to the second device.

10. (Currently Amended) A system according to Claim 9, wherein the second device receives the cryptogram c and ~~implements a decryption method, in order~~ performs the following calculation to decrypt said cryptogram~~, which comprises the performance of the following calculation steps~~:

1. $m_1 = \log_n(c^{\lambda(n)} \bmod n^2).\log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$
2. $w = cg^{-m1} \bmod n$
3. $m_2 = w^{1/n \bmod \lambda(n)} \bmod n$
4. $m = m_1 + nm_2$.

11. (Currently Amended) A system according to Claim 10, wherein the second device ~~implementing said decryption method~~ precalculates the following quantities:

$\alpha_{n,g} = \log_n(g^{\lambda(n)} \bmod n^2)^{-1} \bmod n$, and

$\gamma_n = 1/n \bmod \lambda(n)$,

and stores them secretly in a protected area of a program memory.

12. (Currently Amended) A system according to Claim 10, wherein said second device performs the following calculation ~~steps during said decryption method~~, using the Chinese Remainder Theorem:

1. $m_{1,p} = \log_p(c^{p-1} \bmod p^2)\log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

2. $w_p = cg^{-m1,p} \bmod p$

3. $m_{2,p} = w_p^{1/q \bmod p-1} \bmod p$

4. $m_{1,q} = \log_q(c^{q-1} \bmod q^2).\log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

5. $w_q = cg^{-m1,q} \bmod q$

6. $m_{2,q} = w_q^{1/p \bmod q-1} \bmod q$

7. $m_1 = CRT(m_{1,p}, m_{2,p}, p, q)$

8. $m_2 = CRT(m_{1,q}, m_{2,q}, p, q)$, and

9. $m = m_1 + pqm_2$ where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

and x is any integer.

13. (Previously Presented) A system according to Claim 12, wherein said second device precalculates the following quantities:

$\alpha_{p,g} = \log_p(g^{p-1} \bmod p^2)^{-1} \bmod p$

$\alpha_{q,g} = \log_q(g^{q-1} \bmod q^2)^{-1} \bmod q$

$\gamma_p = 1/q \bmod p-1$

$\gamma_q = 1/p \bmod q-1$

and stores them secretly in a protected memory area of a program memory.

14. (Currently Amended) A system according to claim 10, wherein the ~~decryption method is used for calculating~~ calculation performed in said second device

generates the signature s of a message m and the ~~encryption method is~~ steps executed in the first device are used for verifying said signature.

Claims 15 and 16. (Canceled)

17. (Currently Amended) A system according to Claim [[15]] 2 wherein the second device ~~implements a method of decryption of~~ performs the following calculations to decrypt the received cryptogram c, ~~comprising the performance of the following calculation~~:

$m = \log_n(c^u \bmod n^2).\log_n(g^u \bmod n^2)^{-1} \bmod n$,

where u is an integer that divides (p-1) and (q-1).

18. (Currently Amended) A method according to Claim 17, wherein said second device ~~implementing said decryption method~~ precalculates the quantity:

$\beta_{n,g} = \log_n(g^u \bmod n^2)^{-1} \bmod n$

and stores it secretly in a protected area of a program memory.

19. (Currently Amended) A system according to Claim 17, wherein said second device performs the following calculation steps ~~during said decryption method~~, using the Chinese Remainder Theorem:

1. $m_p = \log_p(c^u \bmod p^2).\log_p(g^u \bmod p^2)^{-1} \bmod p$

2. $m_q = \log_q(c^u \bmod q^2).\log_q(g^u \bmod q^2)^{-1} \bmod q$

3. $m = CRT(m_p, m_q, p, q)$, where $\log_p$ and $\log_q$ are such that

$$\log_i(x) = \frac{x-1}{i}$$

x being any integer.

20. (Currently Amended) A system according to Claim 19, wherein said second device ~~implementing said decryption method~~ precalculates the following quantities:

$\beta_{p,g} = \log_n(g^u \bmod p^2)^{-1} \bmod p$

$\beta_{q,g} = \log_n(g^u \bmod q^2)^{-1} \bmod q$

and stores them secretly in a protected area of a program memory.

21. (New) The method of claim 1 further including the step of calculating the value $\lambda(n) = LCM(p-1, q-1)$, and wherein the private key is generated from the parameters p, q and $\lambda(n)$.

22. (New) A cryptographic communication system with public and private keys generated according to Claim 21, comprising a communication channel and first and second

communicating devices, each device comprising at least one communication interface, data processing means and storage means, wherein said first device executes the following steps to send the number m to said second device

- using the parameters of the public key of the second device to assign the values of the public key to the parameters n and g,

- calculating the cryptogram $c = g^m \bmod n^2$, and

- transmitting said cryptogram over the communication channel to the second device.